Joint Universities Computer Centre Limited
( "JUCC" )
Information Security Awareness Training- Session Two

Information Security- Perspective for Management
# Information Management

## Agenda

- Information Management
- Data Classification
- Data Flow Analysis
- Information Security
- Privacy
- Third-party Management





## Information Management

Information Management is the collection and management of information from one or more sources and the distribution of that information to one or more audiences with the aim of protecting the information based on its business value and associated risks.





## Why protecting information?

- Information is **valuable assets.**
- Because staff need to handle **sensitive and confidential information**, it is necessary to educate employees how to properly secure data.
- Universities have an increasing **dependency on information**
- The **risk** of data being misused or accidentally/ deliberately modified or damaged increases.

## Implementing comprehensive information management in Universities

- Certain types of data must be specially handled to fulfill the university's legal or moral obligations.
- This requires control mechanisms that are **safe** and **easy** to use. Controls are required to protect the **CIA** of data.

**HOWEVER…**



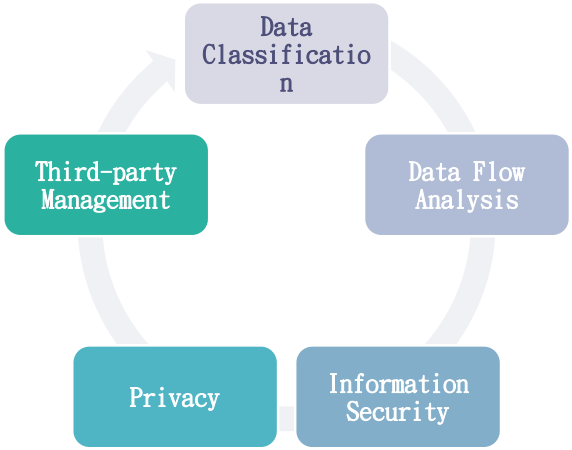


## Challenges

- ***However***, with the decentralised nature of information in universities, management/ information security team may not already have the relevant knowledge of:
  - What data exist in campus;
  - Where they are;
  - Who owns them;
  - What level of protection is required; and
  - How to protect them.

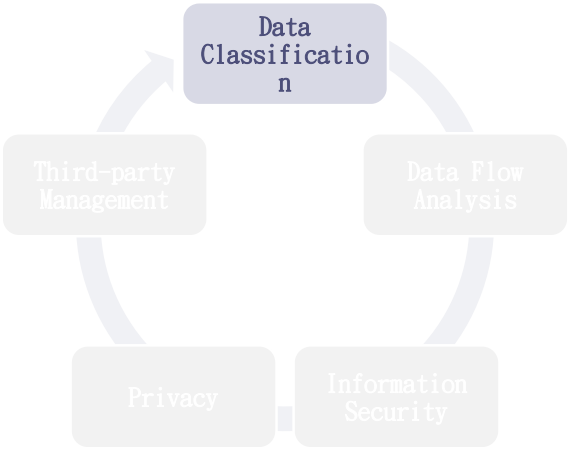










## Data Classification

- Dividing data sources (documents, applications, databases, etc.) into groupings
- Facilitate defining of the level of controls, protection and policies to be applied to support business objectives
- Allow users to apply the appropriate handling procedure according to the classification





## Responsibilities in Data Classification

- **Management** – **provides framework and defines classifications**
- **IT** – provides appropriate infrastructure and support
- **Data owner** – identify & classify data and apply controls

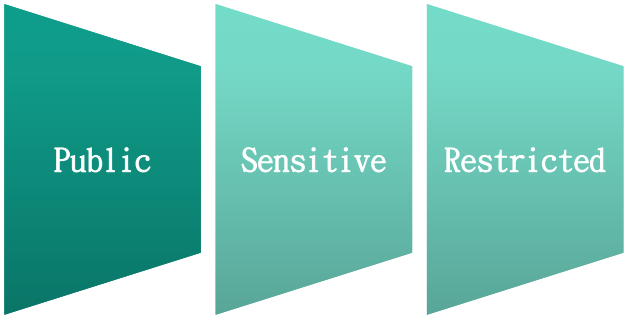
** Data owners are people with the best knowledge of how to identify and classify the data they own **





**For the purpose of handling data appropriately, data is classified by data owners into categories- classification level.**

Classification levels commonly used:

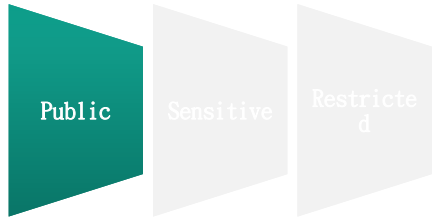






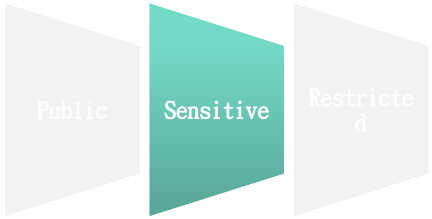

# Public

- Information which may or must be open to the general public.
- It is defined as information with no existing local, national or international legal restrictions on access.
- Example: reports containing generalised information (e.g. summary reports, enrollment reports, degrees conferred reports, etc), or any report that contains only directory information.



## Sensitive

- Information whose access must be guarded due to proprietary, ethical, or privacy considerations.
- This classification applies even though there may not be a civil statute requiring this protection.
- Example: Student ID; Electronic signature.

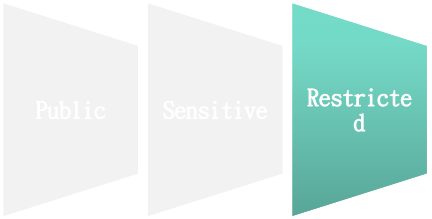






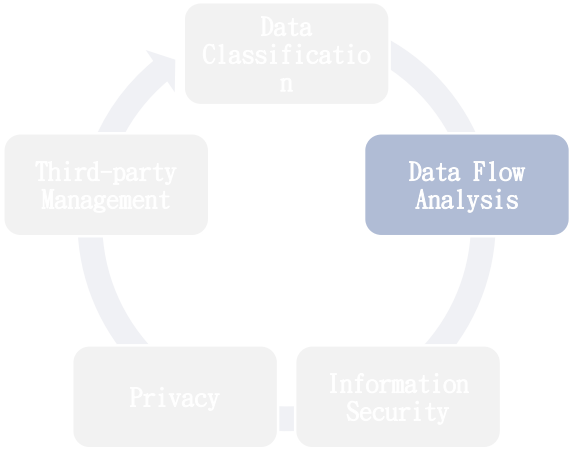

## Restricted

- Information protected because of protective statutes, policies or regulations.
- Data which data owner exercised their right to restrict access.
- Example: Business confidential, secret design/ formula












- Data flow analysis – the process of classifying and managing the flow of information assets within and going out of the institution.
- From Creation to Destruction depending on the relevant business process

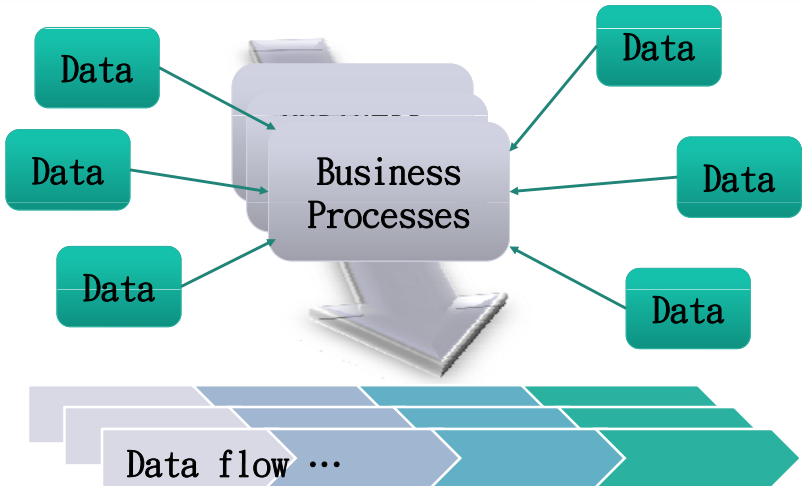
- Examples:

Create ➔ Store ➔ Transfer

Create ➔ Store ➔ Print ➔ Destroy

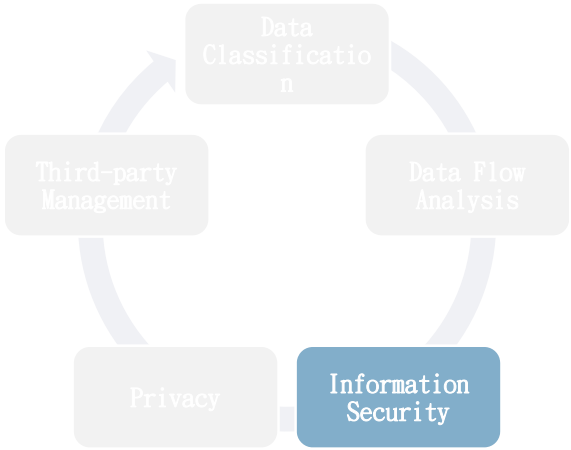
Create ➔ Backup ➔ Archive

## Data Flow Analysis






## Information Management






## Information Security

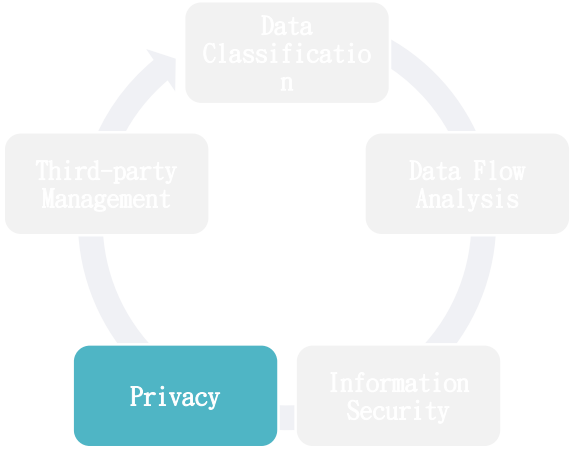
| Create | Access | Disclose | Store | Print | Backup | Destroy |
|---|---|---|---|---|---|---|
| Public | | | | | | |
| Sensitive | | | | | | |
| Restricted | | | | | | |
| Confidentiality | | Integrity | | | Availability | |

Data Handling Guidelines

Information Security Policy



## Information Management



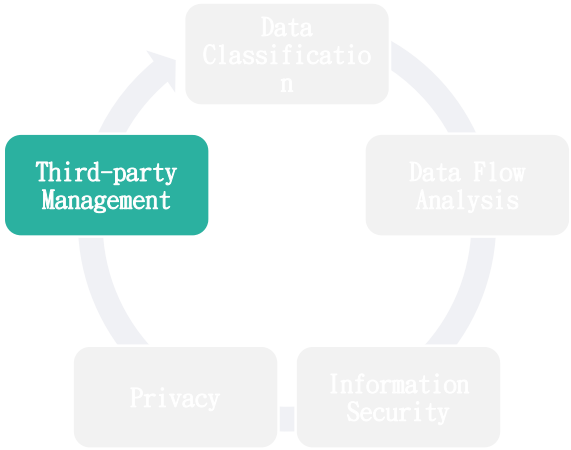
## Privacy Protection

### Responsibilities of Management

- Understand the legal and regulatory requirements
- Assign roles and responsibilities for data owners, data custodian and data users
- Design and enforce proper privacy protection procedures
- Provide adequate training
- Promote privacy protection



## Information Management






## Third-Party Management

### Third-Party

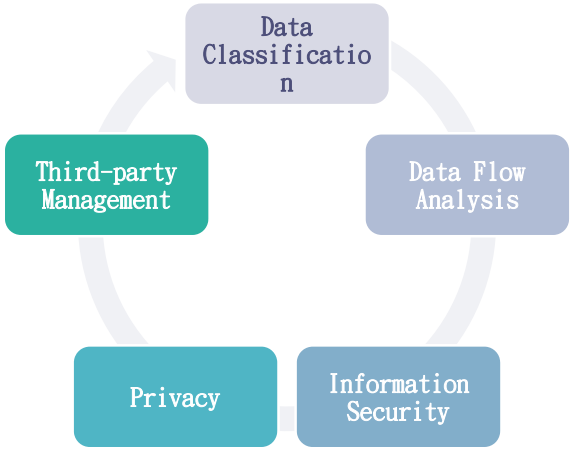
- Outsourced data centres/ information systems
- Third-party data processor (data entry/ destruction)

### Third-Party Management

- Third-party handling policy/ procedures
- Security standard of third-party
- Compliance towards University’s data handling procedures
- Confidentiality/ Non-disclosure agreement
- Audit rights requirements
- Review of third-party performance (security compliance)



## Information Management




Q&A

?